RESPONSE

Claims Status

Claims 1-8 were originally filed in this application. In an Office Action dated December 16, 2004, Claims 1-8 were rejected, and an amendment and response was filed on May 9, 2005 in response thereto. A final Office Action was mailed on August 5, 2005, maintaining the rejection of claims 1-8. In this Amendment and Response, Applicant has cancelled claims 1 and 6-8, amended claims 2-5, and added new claims 9-16. Support for the amendments and new claims can be found at least in the originally filed claims and in the specification at paragraphs [0039], [0032] and [0038]. No new matter has been added.

Rejection of the Specification

In the current Action, the Specification was objected to under 35 U.S.C. 132(a) as introducing new matter into the disclosure. Applicant believes that the above amendment to the Specification addresses this objection and respectfully requests the withdrawal of the objection.

Claim Rejections

Claims 1, 3-6 and 8 have been rejected under 35 U.S.C. 103(a) as being unpatentably obvious over U.S. Patent No. 5,420,866 to Wasilewski ("Wasilewski") in view of U.S. Patent No. 6,735,313 to Bleichenbacher et al. ("Bleichenbacher") and in further view of U.S. Patent No. 6,212,633 to Levy et al. ("Levy").

Claims 2 and 7 have been rejected under 35 U.S.C. 103(a) as being unpatentably obvious over Wasilewski in view of Bleichenbacher, in further view Levy, and in further view of U.S. Patent No. 5,768,381 to Hawthorne ("Hawthorne").

New Claims 9 and 13

Following cancellation of claims 1 and 6 and entry of new claims 9 and 13, claims 9 and 13 will be the only independent claims in this application, all other claims depending therefrom.

Newly presented independent claims 9 and 13 each recite using unique packet tags to encrypt or decrypt secure content at transmission (claim 9) or receipt (claim 13). More specifically, claim 9 recites, in part, "creating a packet key for each data packet" and "encrypting each data packet using the packet key" where the packet key is based on a base key "and unique packet tags assigned to each data packet." Likewise, claim 13 recites, in part, "receiving an encrypted packet stream . . . comprising a plurality of packets" where each packet includes "a unique tag value" and "computing a packet key for each packet based on the unique tag value." As a result, each packet of a given data stream contains information (i.e. the packet tag) packet *uniquely identifies that packet* is used to create encryption and decryption keys. See, for example, paragraphs 0029 and 0032 of Applicants' published application.

The Office Action contends that "Wasilewski discloses a unique tag value [that] is assigned to each packet." Applicant respectfully submits that this interpretation of the packet_ID described in Wasilewski is incorrect, and in fact is directly contradicted by the text of Wasilewski. Wasilewski describes transmitting "different elementary streams" by inserting a packet ID in a header section of each transport packet of the sequence being transmitted. Although Wasilewski characterizes the packet IDs as being unique, they are not unique *at the packet level* as required by the present claims.

Specifically, unlike the claimed packet tags that are unique to each packet and used to generate packet-specific encryption keys, Wasilewski describes "assign[ing] a unique Packet_ID (PID) to each Transport Packet in the sequence that carries the ECMs *for that elementary stream*." Wasilewski goes so far as to provide an example confirming that the packet IDs are the same for each packet within a stream, stating "each Transport Packet in the sequence of Transport Packets that carry the ECMs for video elementary stream 'Video 1' is assigned a PID value of '27'." Col. 15 lines 33-40 and FIG. 3B. The uniqueness of the packet IDs described in Wasilewski is therefore at the stream level, and thus *are the same for each packet* within a specific data stream. Wasilewski does not, therefore, teach or suggest using "unique packet tags"

to generate packet-level encryption and decryption keys as recited in each of the independent claims.

Bleichenbacher also describes methods and systems for delivering encrypted content using a program identifier and a program key. Similar to the stream-level packet IDs of Wasilewski, Bleichenbacher uses a "program key K_p, which may be unique to the program" to encrypt a data stream. Because the program keys used by Bleichenbacher are program specific, Bleichenbacher, like Wasilewski, does not teach or suggest using unique packet-level information (such as the claimed "unique packet tags") to generate packet-specific encryption keys.

Finally, Levy also does not teach or suggest using unique, packet-level information to encrypt or decrypt data streams, instead describing well-known public-private session keys that remain consistent throughout an entire communication session to transmit content among trusted nodes within a network. As such, neither Bleichenbacher nor Levy cure the deficiency of Wasilewski.

Thus, Applicant respectfully submits that independent claims 9 and 13, as well as those claims that depend therefrom, are patentable over the cited references.

CONCLUSION

Applicant respectfully requests that the Examiner reconsider the application and claims in light of this Response, and respectfully submit that the claims are in condition for allowance. If the Examiner believes, in his review of this Response or after further examination, a telephonic interview would expedite the favorable prosecution of the present application, the Applicant's attorney would welcome the opportunity to discuss any outstanding issues, and to work with the Examiner toward placing the application in condition for allowance.

Respectfully submitted,

Date: December 5, 2005
Reg. No. 56,401

Tel. No.: (617) 570-1057
Fax No.: (617) 523-1231

Joel E. Lehrer
Attorney for Applicants
Goodwin Procter LLP
Exchange Place
Boston, Massachusetts 02109
Customer No. 051414